UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

UM MODELO DE SEGURANÇA PARA O SISTEMA DE PRESCRIÇÃO ELETRÔNICA DO HUSM

TRABALHO DE GRADUAÇÃO

Francisco Henrique Lüder Ripoli

Santa Maria, RS, Brasil
2008

UM MODELO DE SEGURANÇA PARA O SISTEMA DE PRESCRIÇÃO ELETRÔNICA DO HUSM

por

Francisco Henrique Lüder Ripoli

Trabalho de Graduação apresentado ao Curso de Ciência da Computação da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de
Bacharel em Ciência da Computação

Orientador: Prof. Dr. Raul Ceretta Nunes

Trabalho de Graduação N° 273
Santa Maria, RS, Brasil
2008

Universidade Federal de Santa Maria
Centro de Tecnologia
Curso de Ciência da Computação

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

UM MODELO DE SEGURANÇA PARA O SISTEMA DE PRESCRIÇÃO ELETRÔNICA DO HUSM

elaborado por
Francisco Henrique Lüder Ripoli

como requisito parcial para obtenção do grau de
Bacharel em Ciência da Computação

COMISSÃO EXAMINADORA:

Raul Ceretta Nunes, Dr.
(Presidente/Orientador)

Antônio Marcos de Oliveira Candia, Msc. (UFSM)

Roseclea Duarte Medina, Drª. (UFSM)

Santa Maria, 15 de dezembro de 2008

AGRADECIMENTOS

Agradeço primeiramente a Deus pela vida maravilhosa que tenho.

Agradeço aos meus pais pela criação que me deram e por todo o suporte para que pudesse chegar até aqui. Agradeço também aos meus irmãos por todos os momentos que passamos juntos.

Agradeço à minha namorada Ellen por todo o carinho e compreensão durante toda a realização deste trabalho. Também por me auxiliar com as figuras aqui contidas.

Agradeço ao meu orientador Raul por todas as conversas, discussões e realizações sobre este trabalho. Agradeço também à Maria Angélica por ser uma excelente colega de sala e quase co-orientadora.

Agradeço a todos colegas que em algum semestre, em alguma matéria, esclarecemos dúvidas, compartilhamos conhecimentos e conseguimos avançar em direção à colação de grau.

Agradeço também a todos que, de alguma maneira, me ajudaram a alcançar essa conquista.

A todos, muito obrigado.

RESUMO

Trabalho de Graduação
Curso de Ciência da Computação
Universidade Federal de Santa Maria

UM MODELO DE SEGURANÇA PARA O SISTEMA DE PRESCRIÇÃO ELETRÔNICA DO HUSM

Autor: Francisco Henrique Lüder Ripoli
Orientador: Prof. Dr. Raul Ceretta Nunes
Local e data da defesa: Santa Maria, 15 de dezembro de 2008.

O Hospital Universitário de Santa Maria (HUSM) dispõe de diversos serviços para a comunidade local e a informatização dos diferentes setores do hospital possibilita um melhor controle das atividades administrativas e clínicas, requerendo a definição de um modelo de segurança. Um modelo de segurança procura identificar possíveis ameaças a um sistema e contém as principais características e formas de combatê-las, servindo como base para o desenvolvimento de sistemas resistentes a elas. Considerando que a segurança dos dados do paciente é um fator chave, este trabalho propõe um modelo de segurança para o sistema de prescrição eletrônica do HUSM.

Adequando-se ao Nível de Garantia de Segurança 1 proposto pelo Conselho Federal de Medicina, o modelo proposto especifica: formas de autenticação; um modelo de controle de acesso baseado em contexto; como deve ser o canal de comunicação entre cliente e servidor; maneiras de garantir a segurança dos dados, tanto em trânsito como armazenados em um sistema de banco de dados; e formas de possibilitar uma auditoria segura no sistema.

Palavras-chave: prescrição eletrônica, segurança da informação, modelo de segurança.

ABSTRACT

Undergraduation Final Work
Undergraduation in Computer Science
Federal University of Santa Maria

A SECURITY MODEL FOR THE ELECTRONIC PRESCRIPTION SYSTEM OF HUSM

Author: Francisco Henrique Lüder Ripoli
Advisor: Raul Ceretta Nunes

The University Hospital of Santa Maria (HUSM) offers different services for the local community and new technologies in all of the sectors of the hospital allows a better control of administrative and clinical activities, requiring a security model definition. A security model tries to identify possible threats to a system and has the main characteristics to fight them, working as a base for the development of a system resistant to these threats. Considering the security of patients' data as a key factor, this work proposes a security model for the electronic prescription system of HUSM.

Matching the requirements of the security guarantee level 1, the proposed model specify: methods of identification and authentication; a model for access control based in context; how the communication between client and server should happen; different ways for guaranteeing the data secure, both data in transit or data at rest; and possibilities of a secure audit.

Keywords: electronic prescription, information security, security model

SUMÁRIO

1 INTRODUÇÃO

O direito do ser humano em ter acesso à saúde e aos cuidados médicos são necessidades fundamentais da sociedade, esta afirmativa é contemplada no Artigo XXV da Declaração Universal dos Direitos Humanos (Organização das Nações Unidas, 2004).

Hospitais de Ensino, vinculados às Instituições Federais de Ensino Superior, são considerados referências do Sistema Único de Saúde nas ofertas de serviços de alta e média complexidade. A informatização hospitalar, hoje pouco disponível, é de extrema necessidade para a implantação de melhorias em processos de gestão-ensino-assistência.

A Portaria Interministerial Nº 1000 de 15/04/2004, no parágrafo XVII (Brasil, 2004), dispõe sobre a proposição de novos modelos de utilização da informação e define que o Hospital de Ensino deve prover de uma estrutura mínima de gestão hospitalar, que inclua rotinas técnicas operacionais, sistema de avaliação de custos e sistema de informação integrados.

A utilização da tecnologia da informação em um hospital de ensino, assistência e pesquisa, pode auxiliar em muito na viabilização econômica da organização. Segundo Gimenes et al. (2006) a adoção de sistemas de prescrição eletrônica auxilia na garantia da qualidade e segurança da assistência dos pacientes hospitalizados, bem como na garantia dos recursos para prestação de serviços.

Sujeita a rasuras, presença de abreviaturas ou nomes comerciais, ou mesmo a ausência de informações como via e freqüência de administração, a prescrição manual apresenta uma série de erros que podem colocar em risco a saúde do paciente e degradar a qualidade da assistência em enfermagem (Winterstein et al., 2004).

Estudos prévios demonstram que na Inglaterra cerca de 15% das prescrições apresentam um ou mais erros (Ridley, Booth e Thompson, 2004) enquanto que nos Estados Unidos este número chega a 19% (Berger, Kichak e Pchak, 2004), podendo ser maior nos hospitais públicos brasileiros. As falhas relacionadas aos medicamentos estão divididas em três etapas e todas elas suscetíveis a erros: prescrição, dispensação e administração. Winterstein et al. (2004) mostraram que 72% dos erros de medicação foram iniciadas durante a prescrição, seguidos pela administração (15%), dispensação (7%) e transcrição (6%).

Para Bates (2000), as prescrições médicas eletrônicas podem aumentar a segurança dos medicamentos, pois são mais estruturadas, são mais legíveis e muitas informações podem ser fornecidas ao prescritor durante o processo de prescrição, possibilitando que o erro seja corrigido no momento da digitação eliminando assim a chance de haver rasuras ou rabiscos que podem vir a dificultar ainda mais o entendimento das informações.

A prescrição eletrônica oferece maior segurança para os pacientes, pois reduz a freqüência de erros (Gimenes et al., 2006), principalmente pela melhor legibilidade da prescrição. Porém a prescrição eletrônica também é chave para a qualidade do atendimento e para a pesquisa clínica. Quando informatizada, a prescrição possibilita a recuperação instantânea de qualquer prescrição armazenada; implementação de prescrição provisória para validação posterior por docente ou contratado; padronização de medicamentos de estoque; facilitação para utilização de nomes genéricos ao invés de nomes comerciais; e verificação de equívocos decorrentes de possíveis erros de digitação.

O Hospital Universitário de Santa Maria (HUSM) é reconhecido como um Centro de Ensino, Pesquisa e Assistência no âmbito das Ciências da Saúde, prestando um serviço de excelência que abrange mais de 100 municípios, desenvolvendo inúmeras ações. Por caracterizar-se como um hospital escola, oferece um campo de ensino prático aos alunos de graduação e pós-graduação da Universidade Federal de Santa Maria (UFSM) em especial aos da área da saúde, permitindo que diversas atividades de cunho teórico e prático sejam realizadas. Outro diferencial que ressalta a importância do HUSM é ser o único hospital da região central que oferece serviços pelo Sistema Único de Saúde (SUS).

São realizadas por semana mais de 1000 prescrições médicas, número considerado alto pelas condições do HUSM e pela forma manual com que elas são realizadas. A manutenção deste modelo tradicional tem impactado negativamente nos processos de ensino, gestão, pesquisa, extensão e assistência da instituição.

Além de um projeto especializado, a prescrição eletrônica no HUSM demanda soluções inovadoras para garantir disponibilidade, integridade e confidencialidade das prescrições. Como exemplo, fraudes eletrônicas podem alterar a prescrição, com vistas à mudança de faturamento ou lesão à pacientes; e defeitos na rede ou nos discos do sistema podem provocar a perda de integridade da informação ou de sua disponibilidade, prejudicando diretamente a assistência ao paciente.

Deve-se então analisar questões de segurança para um modelo de prescrição eletrônica que, sendo adequado a um hospital de ensino público, atenda os requisitos fundamentais: disponibilidade, integridade e confidencialidade.

Esse trabalho tem como objetivo propor um modelo de segurança para o sistema de prescrição eletrônica do Hospital Universitário de Santa Maria (HUSM), a fim de garantir um nível adequado de segurança ao sistema, principalmente em uma instituição hospitalar que tem como princípios a credibilidade e a garantia a uma assistência correta e responsável.

Este trabalho está organizado da seguinte forma: o capítulo 2 apresenta os aspectos legais e tecnológicos da prescrição eletrônica; o capitulo 3 faz uma apresentação geral sobre modelos de segurança e os especifica para a área médica; no capítulo 4 são discutidas as exigências do Conselho Federal de Medicina (CFM) para sistemas eletrônicos de saúde e apontando tecnologias capazes de satisfazê-las. Por fim o capítulo 5 apresenta as conclusões finais.

2 PRESCRIÇÃO ELETRÔNICA

Em um momento onde processos estão sendo informatizados ao máximo, a informatização de sistemas médicos sofre pressões para entrar nessa nova era. Essas pressões existem por inúmeros motivos que podem ser caracterizados como: o desejo de melhorar a assistência médica através do acesso a sistemas de suporte médico; a necessidade de acesso simultâneo a informações por médicos, enfermeiros e administradores; a mobilidade de pacientes; e a possibilidade de suprir pesquisas médicas com informações relevantes (Rindfleisch, 1997).

Segundo Gimenes et al. (2006) a prescrição eletrônica oferece maior segurança para os pacientes, pois reduz a freqüência de erros principalmente pela melhor legibilidade da prescrição. Entretanto, a prescrição eletrônica também pode ser considerada como a chave para alcançar a qualidade do atendimento e conseqüentemente para a pesquisa clínica. Quando informatizada, a prescrição possibilita:

- recuperação instantânea de qualquer prescrição armazenada;
- implementação de prescrição provisória para validação posterior por docente ou contratado;
- padronização de medicamentos de estoque;
- facilitação para utilização de nomes genéricos ao invés de nomes comerciais; e,
- verificação de equívocos decorrentes de possíveis erros de digitação.

Com um sistema de prescrição eletrônica, por meio de sistemas distribuídos, independente de onde o paciente é atendido, se tem uma viabilização do acesso às informações. A disponibilidade delas apresenta vantagens como:

- Prestadores de serviços de saúde possuirão melhores informações sobre o paciente. Estas informações possibilitam uma melhora na qualidade do atendimento ao paciente bem como a redução de custos evitando, por exemplo, que um paciente faça mais de uma vez procedimentos ou exames que já se conheçam os resultados (National Academy of Sciences, 1997).

- Pesquisadores e o Serviço Público de Saúde poderão realizar estudos epidemiológicos mais abrangentes, mais precisos, com benefícios para comunidade científica. Sistemas de assistência médica informatizados possibilitam que centros de tratamento tenham acesso às mais recentes informações de pacientes e também ao suporte para definir o melhor tratamento para cada caso. Pesquisadores e oficiais da saúde terão acesso a mais e melhores informações para seus estudos de doenças e eficácia de tratamentos.
- Gestores possuirão subsídios para uma melhor tomada de decisão na elaboração de padrões para o atendimento à saúde (Rindfleisch, 1997). Com isso é gerada uma facilitação da participação e controle social em decisões políticas na área da saúde, possibilitando um melhor nível de informação sobre a eficácia ou qualidade de sistemas de saúde (Sacardo & Fortes, 2000).

Com a informatização de um sistema de atendimento médico, mesmo com todos os benefícios que podem ser trazidos, são levantadas questões sobre a privacidade do paciente e a confidencialidade de suas informações. A questão de quem pode, ou não, ter acesso a qualquer tipo de dado do paciente é largamente discutida em estudos na área médica. Normas incluídas em leis, projetos complementares e, principalmente, nos códigos de ética profissional definem uma política de acesso aos dados. Essas normas definem obrigações, permissões e proibições a todos os envolvidos em processos na área da saúde (Motta, 2002).

2.1 Aspectos Legais

Informações pessoais do paciente são fornecidas em confidência durante o atendimento ou obtidas através de exames ou procedimentos realizados para diagnóstico ou terapia (Francisconi & Goldim, 1998). Essas informações só interessam ao próprio paciente e são confidenciadas por uma necessidade.

O segredo médico é bastante antigo e vem desde o Juramento de Hipócrates, datado do século V a.C., que diz claramente: *“àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto”* (Juramento de

Hipócrates, 2004).

Com a finalidade de preservar a privacidade do paciente, o silêncio é exigido de médicos. Uma divulgação da vida privada do indivíduo pode provocar prejuízos em seus interesses morais e econômicos (França, 2002). Somente com o consentimento do paciente, seus dados podem ser divulgados (Oliveira, 2001).

A troca de informações entre membros da equipe médica deve se limitar àquelas precisamente necessárias para a realização da atividade em favor do cuidado ao paciente (Sacardo & Fontes, 2000). Informações pessoais do paciente não podem ser livremente acessadas por ninguém, além do paciente ou representante legal. O acesso só deve ser autorizado mediante necessidade profissional de médicos, membros da equipe médica ou profissionais administrativos (Francisconi & Goldim, 1998).

Francisconi & Goldim (1998) recomendam o estabelecimento de “medidas para evitar que pessoas sem qualquer envolvimento com o paciente, ou que não necessitem saber detalhes imprescindíveis à sua atividade profissional, venham a ter informações sobre o mesmo”.

As instituições têm o dever de manter o sistema seguro, com uma ininterrupta evolução de normas e identificação e controles de acesso de usuários, e possuir uma política de controle de acesso clara e explícita (Al-Salqan,1998).

Uma questão importante e decisiva para a elaboração das políticas de segurança é possuir o conhecimento de quem tem o direito de acesso aos dados de saúde, ou seja, o controle de acesso. Para essa definição devem ser consultados todos os envolvidos no processo da saúde, tendo o Governo como regulamentador. Normalmente essa discussão é longa como mostrada por Varga (1980).

Sabendo do desafio em formular tais políticas de segurança, este trabalho tem como preocupação principal a adequação à legislação, não esquecendo aspectos legais ou funcionalidades que o sistema puder possuir. O sistema deverá ser analisado previamente para uma aceitação perante a legislação e normas.

2.1.1 Legislação Internacional

A Organização das Nações Unidas (ONU) exige segurança dos arquivos, não-discriminação dos dados pessoais, respeito aos princípios de confidencialidade,

declarações e legitimidade das informações. Os Estados Membros da Organização de Cooperação e de Desenvolvimento Econômico (OCDE) são recomendados a coletar apenas os dados relevantes para o tratamento do paciente e que não causem constrangimentos.

Desde 1995, na Europa, existem ações para conciliar as normas. Na França a lei nº 78-17 de 6 de Janeiro de 1978 trata questões de saúde relativas à informática, aos arquivos e liberdades (Varga, 1980).

Segundo Kfouri Neto (2003) a Associação Médica Mundial (AMM), fundada em 1947, emitiu uma série de resoluções e declarações. A Declaração de Genebra foi adotada pela AMM em 1948, tornando, posteriormente, o juramento médico adotado pelo Código de Ética da AMM. No juramento estão diversas responsabilidades como o respeito aos dados confiados pelo paciente, mesmo após sua morte.

A Declaração de Helsinque, declaração de princípios éticos para pesquisa médica, foi adotada em 1964 pela AMM (Varga, 1980). Essa foi revisada em 1975 e em 2000. São considerados como fatores principais para a preservação da integridade a privacidade e o consentimento informado.

2.1.2 Legislação Brasileira

Da Constituição Federal de 1988, em seu artigo 5º, inciso X, tem-se que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Segundo (Oliveira, 2001) o sigilo não é apenas de interesse privado, mas sim de toda população, pois, para a sociedade é importante que se possa confiar informações privadas sem preocupar-se com a divulgação pública das mesmas. O dever de sigilo é previsto no Código de Ética Médica, do Conselho Federal de Medicina, artigo 11:

> *O médico deve manter sigilo quanto às informações confidenciais que tiver conhecimento no desempenho de suas funções. O mesmo se aplica ao trabalho em empresas, exceto nos casos em que seu silêncio prejudique ou ponha em risco a saúde do trabalhador ou da comunidade (Código de Ética Médica, artigo 11, Conselho Federal de Medicina).*

É dever do médico garantir a confidencialidade, ou seja, o médico é responsável para que informações dadas em confidência não sejam reveladas sem autorização prévia (Sacardo & Fortes, 2000). O próprio Código de Ética Médica proíbe, no artigo 102, o médico de “revelar fato que tenha conhecimento em virtude do exercício de sua profissão”, com a exceção de que a divulgação pode acontecer se “por justa causa, dever legal ou autorização expressa do paciente” (Conselho Federal de Medicina, 1996, p. 27). “o que se proíbe é a revelação ilegal que tenha como motivação a má-fé, a leviandade ou o baixo interesse” afirma França (2002).

Duas portarias, nº. 1.638/2002 e nº. 1.639/2002, foram aprovadas pelo Conselho Federal de Medicina normalizando o uso de sistemas informatizados, demonstrando uma preocupação com aspectos legais e éticos, procurando garantir autenticidade, integridade, confidencialidade, privacidade, auditagem, assinatura eletrônica e guarda de documentos.

Segundo França (2002), as instituições de saúde devem estabelecer critérios para uso e revelação de dados pessoais procurando omitir ao máximo detalhes irrelevantes. Sacardo e Fortes (2000) entendem que a troca de informações deve se limitar ao mínimo necessário para um atendimento de qualidade. Francisconi & Goldim (1998) recomendam o estabelecimento de *“medidas para evitar que pessoas sem qualquer envolvimento com o paciente, ou que não necessitem saber detalhes imprescindíveis à sua atividade profissional, venham a ter informações sobre o mesmo”.* Os autores também observam que as instituições devem manter o sistema seguro, com aprimoramento das normas e do controle de acesso.

O Manual de Requisitos de Segurança Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (S-RES) (CFM e SBIS, 2007) foi idealizado e elaborado pelo Conselho Federal de Medicina juntamente com apoio técnico da Sociedade Brasileira de Informática e Saúde (SBIS), e sua criação teve como ponto de partida para a sua elaboração as solicitações de pareceres dos quais questionavam a legalidade de sistemas informatizados que capturam, armazenam, manuseiam e transmitem dados do atendimento a saúde. Este documento reúne o detalhamento dos requisitos de segurança, além de conteúdo e funcionalidade que um S-RES deverá atender para estar em conformidade com as resoluções Nº. 1638 e 1639 do CFM de 2002.

2.2 Aspectos Tecnológicos

Com o crescente avanço na utilização de sistemas de informação hospitalar, manter a privacidade do paciente não é de responsabilidade exclusiva dos profissionais administrativos e da saúde. Os sistemas desempenham um papel importante, possuindo também muitas responsabilidades para garantir o uso ético e legal da tecnologia (Al-Salqan, 1998).

Objetivando limitar as ações realizadas por usuários, evitando assim a quebra de privacidade com acessos não autorizados ou desnecessários, o controle de acesso é importante no mantenimento de informações do paciente.

Relatórios médicos possuem diversas informações que em nada prejudicariam se fossem acessadas indevidamente, como por exemplo: altura, peso, pressão arterial, entre outros. Por outro lado, os mesmos relatórios podem possuir informações de quem e como o paciente é. Tópicos como fertilidade, aborto, problemas emocionais, doenças sexualmente transmissíveis, AIDS e outros podem aparecer e o acesso a essas informações deve ser controlado, pois qualquer divulgação dela pode causar prejuízos (Rindfleisch, 1997).

Um sistema online tem por objetivo compartilhar informações entre agentes autorizados possibilitando um melhor diagnóstico, evitando a duplicação de testes arriscados/caros. Medidas de segurança em sistemas médicos devem ser definidas e integradas de maneira racional. Tais medidas devem ser tomadas levando em conta os riscos que podem ser evitados, os benefícios trazidos para pacientes e entidades e seus custos operacionais (Rindfleisch, 1997).

Para entender os riscos de uma divulgação de informações é necessário entender que os dados médicos de um paciente são utilizados em um consultório, clínica ou hospital e depois servem para uma variedade de funções administrativas (Figura 1). São, por exemplo, enviados para seguradoras para justificar o pagamento de serviços e detectar fraudes. Os riscos então podem ser generalizados em:

- Riscos dentro das instituições médicas:
    - Divulgação acidental (equipe médica comenta sobre um caso e a conversa pode ser ouvida por terceiros);
    - Curiosidade (membro da equipe abusa do nível de acesso e obtém informação para uso próprio);
    - Suborno (dados são divulgados intencionalmente para terceiros).

- Riscos de usuários secundários:
  - principalmente nos setores administrativos, funcionários com acesso a informações médicas podem utilizá-las em benefício próprio.
- Invasão ao sistema de informação:
  - antigos funcionários;
  - pacientes insatisfeitos;
  - invasores de rede.

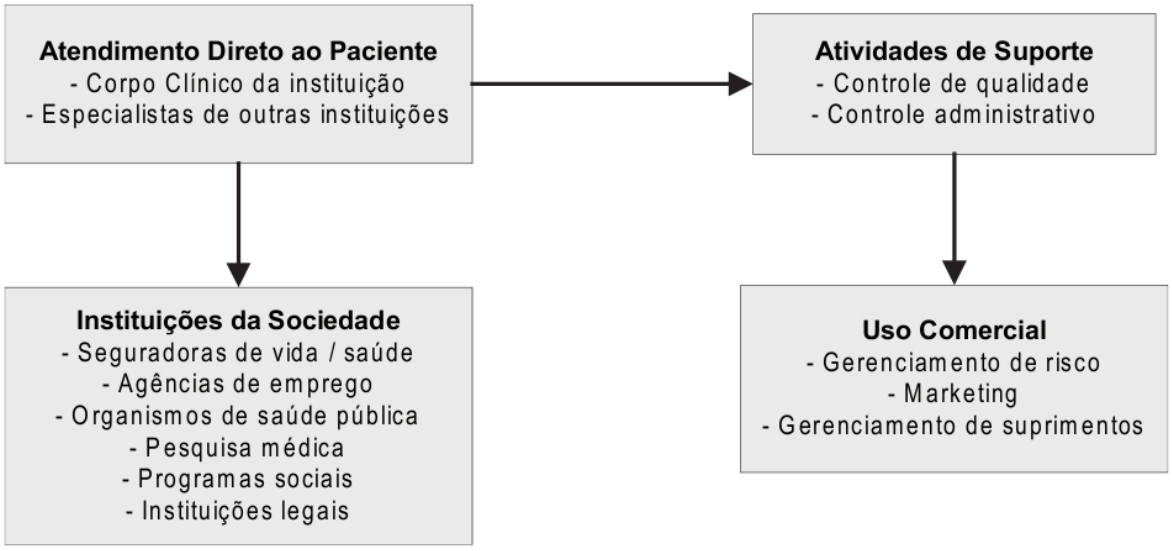

Figura 1 - Exemplos de entidades que acessam informações do paciente (Kobayashi, 2007)

Pode-se observar que há uma grande preocupação para que dados médicos sejam utilizados somente em casos onde serão providos cuidados ao paciente, não podendo ser divulgados em nenhuma outra situação.

Duas questões dificultam a definição de modelos de controle de acesso em ambientes distribuídos. A primeira se refere a quando liberar, ou não, o acesso ao sistema médico. O controle de acesso não pode prejudicar o andamento do atendimento ao paciente, negando o acesso a um usuário legítimo.

Da mesma maneira, o sistema não pode expor os dados do pacientes a pessoas não autorizadas, exceto por determinações legais. Projetar o controle de acesso conciliando casos como esses não é usual (Motta, 2003). Desta forma, é necessária a construção de um modelo para a definição de políticas de controle de acesso onde uma autorização é dada de acordo com a necessidade e direito do usuário.

A segunda questão é relativa a administração dessa política pois o sistema pode possuir características como a composição por aplicações diversas, acessos a bancos de dados distintos e ambientes heterogêneos (Smith & Eloff, 1999).

Para atender essas questões, uma opção é a adoção de arquiteturas de softwares abertas e distribuídas, suportando assim a administração de políticas de autorização e o controle de acesso de maneira simples e efetiva. Atinge-se o objetivo quando se apresenta uma interoperabilidade de sistemas e uma administração unificada (Beznosov, 2000), aliado ao isolamento da lógica de autorização. Com isso, alterações efetuadas na política de controle de acesso não implicam em mudanças no código na aplicação.

3 MODELO DE SEGURANÇA

A segurança é um conceito intuitivo (Kobayashi, 2007), mas ao mesmo tempo extremamente vago por sua vastidão de aspectos que são compreendidos. Neumann (2005) salienta alguns casos reais de riscos em termos de segurança na área médica em diferentes aspectos, incluindo aspectos físicos, que prejudicaram em maior ou menor grau o atendimento aos pacientes. Uma análise em termos de segurança deve ser bastante ampla, levando-se em consideração o contexto no qual a segurança é mencionada.

Sob aspectos em sistemas distribuídos, a segurança pode ser atingida se ela existe nos processos e nos canais de comunicação usados para sua interação, protegendo desta forma os objetos que são encapsulados contra acesso não autorizado (Coulouris, 2005).

Quanto aos canais de comunicação, deve-se ver a segurança dos mesmos em termos de ataques, pois sendo uma rede aberta pode haver ataques externos de usuários malfeitores. Existem ameaças aos processos, ameaça aos canais de comunicação e sobrecarga de uso do recurso. Pode-se ter cópia de mensagens, inserção de mensagens falsas e ataques de volume de requisição exagerada. Uma forma de proteger os canais de comunicação é com o uso de criptografia e autenticação de acesso.

O uso de sistemas de informação em rede vem mudando a forma de disponibilização das informações e com isso tornando a utilização destes recursos de fácil acesso. Essa realidade criada coloca a necessidade de prezar pela segurança da informação, visto que a chance de se tornarem vulneráveis a ameaças é grande e por essa razão se torna essencial a criação de mecanismos de segurança que tenham o intuito de prevenir acessos não autorizados aos recursos e dados destes sistemas (CFM, 2002).

A segurança é a base para que as instituições de saúde forneçam um serviço de credibilidade, organizado e controlado. Uma prestação de serviço eficiente no funcionamento hospitalar está atrelada a tecnologias e estas devem proporcionar, conforme (NBR, 2005):

• Confidencialidade – A informação somente pode ser acessada por pessoas

explicitamente autorizadas; é a proteção de sistemas de informação impedindo que pessoas não autorizadas tenham acesso ao mesmo.

• Disponibilidade – Toda informação deve estar disponível no momento em que a mesma for necessária;

• Integridade – A informação deve ser encontrada em sua forma original desde o momento em que foi armazenada; é a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

3.1 Aspectos Gerais do Modelo de Segurança

O compartilhamento de recursos é o principal fator para a utilização de sistemas distribuídos. Sua arquitetura pode ser descrita por objetos encapsulados por processos e a disponibilização dele em um sistema através de comunicação com outros processos. “A segurança de um sistema distribuído pode ser obtida tornando seguros os processos e os canais usados por suas interações e protegendo contra acesso não autorizado os objetos que encapsulam” Coulouris (2005), definindo o princípio básico de modelos de segurança.

Como mostra a figura 2, um servidor gerencia objetos para usuários. Executando programas clientes os usuários enviam invocações para o servidor, realizando operações sobre seus objetos. O servidor executa a operação solicitada e retorna o resultado para o cliente.

Usuários podem possuir restrições no uso ou acesso a determinados objetos em um sistema. Dados privados de um usuário, como por exemplo o correio eletrônico, não podem ser acessados por outros. Já sua página, um objeto compartilhado, é de livre acesso. Para garantir isso, direitos de acesso definem quem pode, ou não, acessar ou executar operações sobre determinados objetos.

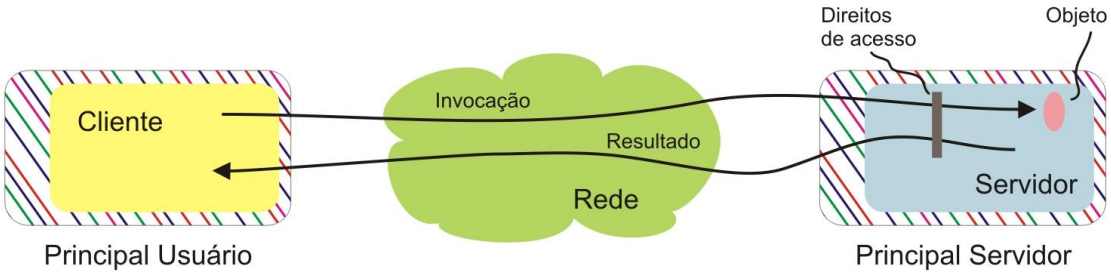

Figura 2 - Objetos e principais

Assim, deve-se ter o usuário no modelo de segurança para garantir o direito de acesso. A cada invocação, Coulouris (2005), associa um tipo de autorização específico, chamada de *principal*. Um principal pode ser o usuário solicitando um objeto ou um servidor retornando o resultado, como mostrado na figura 2.

No servidor, é verificada a identidade de cada principal responsável por cada invocação. Com isso pode conferir a existência de direito de acesso aos objetos e às operações solicitadas. Da mesma forma, o cliente pode verificar se o principal realmente veio do servidor responsável.

A interação dos processos, realizada através de troca de mensagens, os expõem a ataques. Como o acesso ao serviço de comunicação é livre, quaisquer dois processos podem interagir criando uma grande ameaça à integridade das informações.

Sistemas financeiros, médicos e outros que manipulam dados confidenciais são, muitas vezes, desenvolvidos para funcionar de maneira distribuída, sujeitos a ataques externos, tendo assim a integridade ameaçada por violações de segurança.

Um invasor poderia ser um computador autorizado a estar ligado na rede e pode realizar ataques enviando qualquer mensagem para qualquer processo e ler ou copiar qualquer mensagem entre dois processos, como observado na figura 3. Um atacante pode então ameaçar os processos, ameaçar o canal de comunicação ou provocar a negação de serviços.

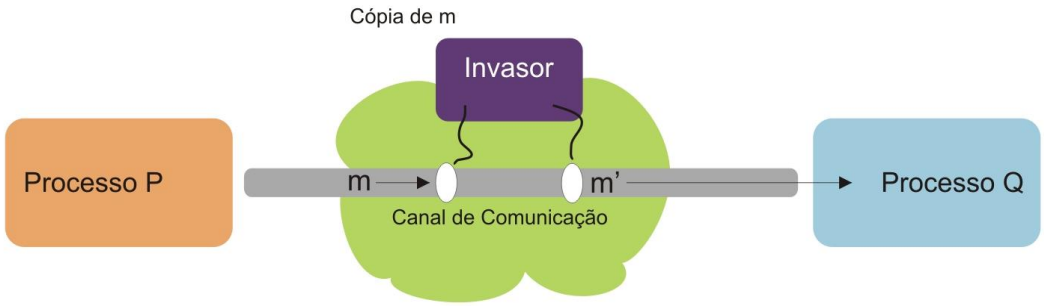

Figura 3 - O invasor

3.1.1 Ameaças aos processos

Um processo que fica “ouvindo” a rede, esperando pedidos de qualquer outro processo do sistema distribuído, pode receber uma mensagem e não pode garantir a identidade de quem a enviou. O endereço do computador é incluído no cabeçalho de cada mensagem em protocolos de comunicação, como, por exemplo, o IP. Com isso, é fácil para um atacante falsificar um endereço e criar uma nova mensagem. Assim uma ameaça ao funcionamento de clientes e servidores é criada, pois não se pode ter certeza da origem da mensagem.

Servidores podem receber mensagens criadas por um invasor solicitando a leitura de um determinado dado. Mesmo exigindo a inclusão da identidade do principal na mensagem, o invasor pode criá-la com uma identidade falsa e enviar ao servidor que, não tendo garantias da identidade, não saberá decidir entre liberar o acesso ao dado ou não.

Os clientes podem receber mensagens, pensando estar recebendo do servidor, quando na verdade estão vindo do invasor. Isso ocorre porque o cliente pode não saber identificar onde a mensagem foi originada. O invasor estaria, nesse caso, utilizando-se de uma técnica chamada *spoofing* que é, na prática, o roubo de identidade.

3.1.2 Ameaças aos canais de comunicação

Conforme Coulouris (2005), ao utilizar o tráfego da rede e de seus sistemas secundários, como por exemplo, roteadores, um invasor pode alterar, copiar ou injetar mensagens. A integridade do sistema é comprometida por essa ameaça, pois, por exemplo, dados de um usuário podem ser enviados para outro, ou mensagens falsas serem introduzidas na rede.

Em um sistema bancário, por exemplo, se o canal de comunicação não for seguro, uma mensagem que ordena a transferência de dinheiro de uma conta para outra pode ser armazenada pelo invasor e reenviada ao servidor duplicando a operação. Com a utilização de canais de comunicação seguros, através de criptografia e autenticação, essas ameaças podem ser anuladas.

A criptografia é estudo de técnicas para transformar dados legíveis em dados

“embaralhados”. O embaralhamento dos dados, dado a partir de chaves ou “segredos”, torna o dado ilegível para todos aqueles que desconhecem a chave para desembaralhar (Nakamura & Geus, 2007).

A autenticação é a comprovação de identidade. Isto é evidenciado quando em uma mensagem a autenticação prova a identidade de quem a enviou, utilizando criptografia e segredos compartilhados. Em um pedido de leitura um servidor decifraria o pedido, que foi cifrado com uma chave secreta compartilhada entre o servidor e o solicitante, e verificaria se a identidade do solicitante é de fato correspondida.

Um canal de comunicação seguro, construído para a comunicação de dois processos, é fundamentado na criptografia e autenticação (Coulouris, 2005). Podem-se citar como exemplos de canais seguros as *Virtual Private Networks* (VPNs) e o protocolo *Secure Sockets Layer* (SSL). Com um canal seguro para a comunicação entre dois processos (figura 4) tem-se garantida a privacidade e a integridade dos dados transmitidos.

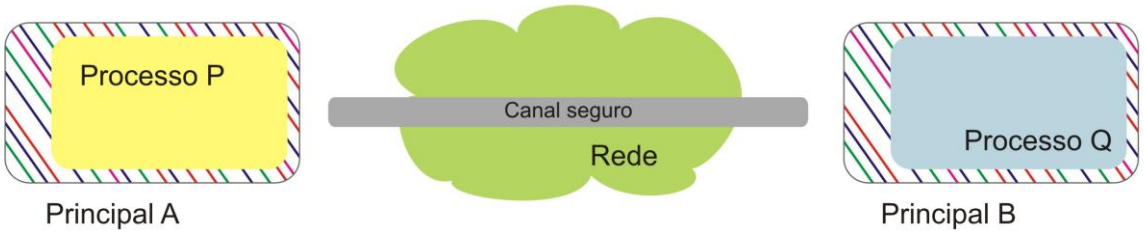

Figura 4 - Canal seguro

3.1.3 Negação de Serviço

Um ataque de negação de serviço – *Denial of Service (DoS)* – é caracterizado por uma tentativa explícita de invasores de evitar que um usuário legítimo de um serviço o utilize. A partir de transmissões incessantes de mensagens, gera-se um grande tráfego na estrutura de rede na tentativa de quebrar a conexão entre dois computadores, além de não deixar que um computador tenha acesso a um determinado serviço. Em geral, esses ataques são feitos procurando impedir, ou retardar, o acesso de usuários a um sistema (Nakamura & Geus, 2007).

3.2 Segurança na Área Médica

Diferentemente de dados em papel, onde o controle de acesso é feito de maneira manual, tecnologias de segurança são partes fundamentais em sistemas *online* e oferecem um grande número de vantagens. Os principais objetivos da segurança da informação em sistemas de saúde são:

- Garantir a **privacidade** dos pacientes e a confidencialidade de dados médicos (prevenção de uma divulgação não autorizada);
- Garantir a **integridade** dos dados (prevenir os dados de serem modificados sem autorização); e
- Garantir a **disponibilidade** dos dados para pessoas autorizadas (prevenção de falhas no sistema)

A privacidade das informações levanta a questão do controle de acesso e a aplicação de criptografia para transmissão e armazenamento dos dados. Para garantir a integridade é necessária a autenticação e autorização do usuário no sistema. Já para garantir disponibilidade são usadas ferramentas de redundância de sistemas e dados, bem como mecanismos de backup.

Segundo Rindfleisch (1997), as tecnologias aplicáveis a esses casos vêm de pesquisas em sistemas distribuídos em computação e, no seu maior nível, possuem cinco funções fundamentais:

- Disponibilidade e integridade: Garantir que informações precisas e atualizadas estejam disponíveis quando necessárias e em lugares apropriados.
- Auditoria: Auxilia que prestadores de serviço de saúde sejam responsáveis por seus acessos e no uso das informações.
- Definição de perímetro: O conhecimento e o controle dos limites de acessos confiáveis ao sistema de informação, nos aspectos físicos e lógicos.
- Limitação de acesso por perfil: Limitar o acesso a classes de usuários para que somente os dados necessários para o atendimento ao paciente sejam disponibilizados.
- Controle: Controle efetivo sobre todos os aspectos da informação.

Resumidamente, na Tabela 1, têm-se uma listagem de intervenções, suas funções e sua relação com a proteção da privacidade. Dividida em três grandes

categorias:

- Dissuadores: Dependem do comportamento ético dos profissionais e provém lembretes para reforçar os padrões;
- Obstáculos: Controlam diretamente a habilidade do usuário em obter um dado e têm como objetivo restringir o acesso para somente as informações que ele necessita e tem o direito de saber; e
- Precauções na gerência do sistema: Involve uma pesquisa pró-ativa em um sistema a fim de garantir que fontes de vulnerabilidades conhecidas sejam eliminadas.

Tabela 1 - Tecnologias aplicáveis para a gerência da segurança de informação

INTERVENÇÃO	FUNÇÃO
Dissuadores	
Alertas e lembretes	Reforçar questões éticas
Auditoria	Alertas no acesso a documentos
Obstáculos	
Autenticação	Determina quem está conectado
Autorização	Determina quem pode acessar que informação
Gerência de integridade	Garante que a informação é a correta
Assinaturas digitais	Validação de documentos
Criptografia	Prevenção de “escutas”
Firewalls e gerências de sistemas de rede	Define o perímetro do sistema e meios de acesso
Ferramentas de gerência de direitos	Controla a distribuição da informação e o acesso
Precauções na gerência do sistema	
Gerência de software	Proteger contra vírus, cavalos de tróia, etc.
Ferramentas de análise de vulnerabilidades do sistema	Detectar vulnerabilidades desconhecidas

Ainda segundo Rindfleisch (1997), foi mostrado que os dissuadores (alertas, lembretes e educação do usuário) são muito efetivos ao reforçar o comportamento

ético da grande maioria dos profissionais de assistência médica. A auditoria também demonstra ser muito efetiva, pois sabendo que o sistema vai registrar a identidade, os horários, e as circunstâncias de todos os acessos dos usuários às informações, e que esses registros de acessos serão revistos regularmente, usuários vão pensar duas vezes antes de usar seus privilégios.

Obstáculos tecnológicos também são muito eficientes. Eles garantem a autenticação do computador e do usuário, garantem que só se tenha acesso aos dados a que se tem direito baseado em identidade e função na equipe médica. *Firewalls* garantem a gerência do perímetro e limitam os modos e protocolos de acesso.

Precauções na gerência do sistema são fundamentais e utilizam da experiência e de conhecimentos acumulados pela comunidade sobre vulnerabilidades de segurança. É feita uma prevenção contra a intrusão de programas como vírus, cavalos de tróia, ou outros que podem prejudicar o sistema.

Na área médica a importância da segurança é garantir a confidencialidade, integridade e disponibilidade das informações. Mais do que isso, é garantir a continuidade do negócio e mitigar os riscos de questões judiciais demonstrando e provendo boas praticas em processos. Para ser efetiva, a segurança deve estar integrada com procedimentos padrões como, por exemplo, a NBR/ISO 17799 e NBR/ISO 27001.

3.2.1 O Papel dos Padrões

Padrões são característica essencial em uma área pouco regulamentada como a computação. Quando há a combinação de computação com a área da saúde, padrões são requisitos fundamentais (Williams, 2006). Por exemplo, a combinação de informações sigilosas e tecnologia móvel representa um grande aumento na complexidade da segurança das informações.

Leis regulam o uso, a coleta e o proprietário de um dado e são usadas para proteger a integridade e o sigilo da informação (Pfleeger, 1997). As leis, normalmente, objetivam a responsabilidade depois do evento (coleta de dados, por exemplo). Padrões são práticas reconhecidas pela qualidade e podem ser usados como medida de comparação.

A NBR/ISO 17799, do ano 2000, foi desenvolvida para dar suporte no desenvolvimento de planos de segurança e revisada em 2005 para cobrir tecnologias recentes e o *e-commerce*. Por ser um guia de boas práticas, a NBR/ISO 17799 não é utilizada para certificação. Para isso existe o padrão NBR/ISO 27001 que possibilita a certificação e especifica requisitos para a implementação de segurança customizável para cada organização.

Utilizando a NBR/ISO 27001 como um de seus referenciais, o Conselho Federal de Medicina aprovou, através da resolução numero 1.821, a criação do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES). Este manual foi elaborado a partir de uma colaboração do CFM e da Sociedade Brasileira de Informática em Saúde, visando aprofundar aspectos técnicos sobre a substituição do papel pelo formato eletrônico.

O processo de certificação SBIS/CFM classifica os S-RES em dois Níveis de Garantia de Segurança da Informação (NGS):

• **NGS1** - categoria constituída por S-RES que não contemplam o uso de certificados digitais ICP-Brasil para assinatura digital das informações clínicas, conseqüentemente sem amparo para a eliminação do papel e com a necessidade de impressão e a posição manuscrita da assinatura;

• **NGS2** - categoria constituída por S-RES que viabilizam a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. Para atingir o NGS2 é necessário que o S-RES atenda aos requisitos já descritos para o NGS1 e apresente ainda total conformidade com os requisitos especificados para o nível de garantia dois.

A informatização de sistemas no HUSM não eliminará, inicialmente, a utilização de papel, e com isso, enquadra-se o sistema de prescrição eletrônica no NGS1.

Nesse nível são definidos onze itens de segurança, com respectivos subitens, nos quais os S-RES devem estar enquadrados. Alinhando estes itens do manual com a abordagem sistemática proposta por Blobel e Roger-France (2001), um modelo de segurança deve manter o foco em seis desses itens:

1. Identificação e autenticação de usuário:
    - métodos de autenticação;

- segurança de senhas;
- controle de tentativas; e
- proteção dos parâmetros de autenticação.

2. Autorização e controle de acesso:
   - controle de acesso ao S-RES;
   - gerenciamento de usuários; e
   - configuração de controle de acesso;
3. Disponibilidade do RES:
   - cópia de segurança; e
   - verificação de integridade na recuperação de dados.
4. Comunicação remota:
   - segurança na comunicação entre cliente e servidor;
   - controle de acesso do cliente ao servidor;
   - restrição de dados transmitidos;
   - segurança na comunicação entre componentes; e
   - controle de acesso entre componentes.
5. Segurança de dados:
   - restrições para transmissão e exportação;
   - impedimento de exclusão e alteração;
   - impedimento de acesso ao banco de dados; e
   - dados de identificação do paciente criptografados.
6. Auditoria:
   - auditoria de acesso;
   - trilhas de auditoria; e
   - restrição de acesso às trilhas de auditoria.

4 MODELO DE SEGURANÇA PARA O HUSM

Os seis itens de segurança citados no capítulo anterior são explorados neste. Foram realizados estudos sobre alternativas para garantir a segurança exigida pelo CFM compondo um modelo de segurança para o HUSM.

O modelo de segurança para o sistema de prescrição eletrônica do HUSM (figura 5) tem como principal objetivo alinhar as necessidades do hospital às exigências do CFM para certificação NGS1, garantindo assim requisitos básicos de segurança: disponibilidade, integridade e confidencialidade.

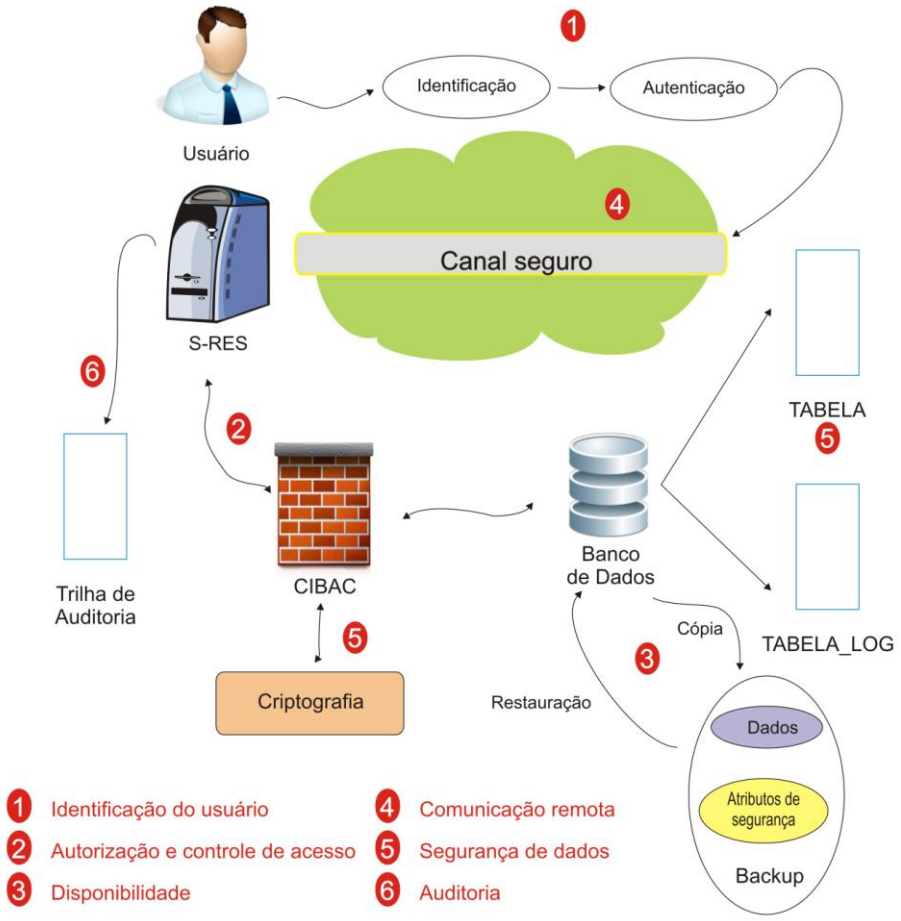

Figura 5 - Modelo de segurança

4.1 Identificação do Usuário

Todo usuário deve ser identificado e autenticado antes de qualquer acesso a dados do S-RES. A identificação e autenticação do usuário, segundo o Manual de Certificação para S-RES, podem utilizar de métodos tracionais como usuário e senha, ou métodos mais seguros como biometria. Quando for utilizado o método de usuário e senha, o manual faz as seguintes exigências:

1. A senha deverá ter, no mínimo, oito caracteres dos quais, no mínimo, um deverá ser não alfabético.
2. O S-RES deverá obrigar o usuário a trocar a senha periodicamente, num período máximo configurável.

Segundo Renaud (2004) sistemas que apresentam essas características, senhas longas e obrigatoriedade de alteração, possuem, em sua equipe de suporte, metade dos chamados para atender usuários que não conseguem realizar a autenticação, principalmente pelo esquecimento da senha. Um sistema médico deve possuir mecanismos para que se tenha um alto nível na garantia de segurança, mas não pode impedir um profissional da equipe de saúde em desempenhar seu papel.

Jain et al. (2004) mostra que um sistema de autenticação por biometria deve ser universal, onde cada pessoa possua a característica; único, onde não existam duas pessoas com a mesma característica; permanente, onde a característica não mude ou possa ser alterada; e coletável, quando é de fácil disponibilidade para um sensor e facilmente quantificável. Com um alto grau de certeza, a utilização de biometria pode garantir a autenticidade da identificação (Jain et al. 2004).

Conforme a tabela 2 pode-se observar que apenas a impressão digital, a íris e a retina possuem uma unicidade alta, característica importante para garantir que somente usuários legítimos tenham acesso ao sistema. Para uma escolha entre as três, deverá ser identificada a que melhor se encaixa em custo/benefício para o hospital e também a possibilidade de integração com o sistema próprio do HUSM.

Ainda no item de identificação do usuário, o Manual de Certificação para S-RES exige que o sistema bloqueie um usuário após um número máximo de tentativas inválidas de *login* (figura 6).

Tabela 2 - Comparação de tecnologias de biometria (Adaptado de Jain, 2004)

Tipo	Universalidade	Unicidade	Permanência	Facilidade de coleta	Facilidade de fraude
Face	alta	baixa	média	alta	alta
Impressão Digital	média	alta	alta	média	baixa
Íris	alta	alta	alta	média	baixa
Retina	alta	alta	média	baixa	baixa
Assinatura	média	baixa	baixa	alta	alta
Voz	média	baixa	baixa	média	alta

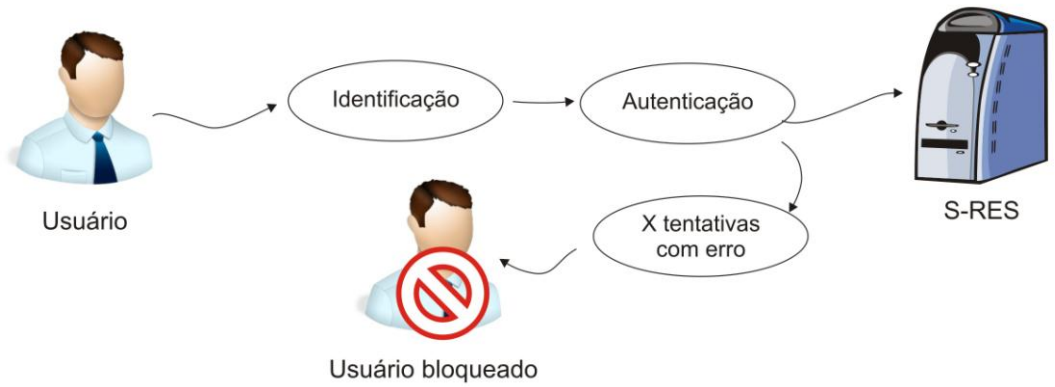

Figura 6 - Somente usuários identificados e autenticados poderão acessar o sistema. Tentativas consecutivas de acesso com erro bloquearão o usuário

4.1.1 Análise Parcial

Em um sistema de prescrição eletrônica, onde dados pessoais e clínicos de pacientes estão disponíveis, a identificação e a autenticação dos usuários que acessam essas informações é requisito fundamental para garantir a confidencialidade desses dados. No entanto, ao se buscar uma solução para atender esse requisito foi sugerido um maior prazo de validade das senhas utilizadas para a autenticação usuário/senha, e a combinação desta com a biometria. Esta definição se justifica pelo número comprovadamente atestado ao qual já fora mencionado na seção 4.1, de incidentes decorridos pela determinação de um período menor de validade de usuário/senha. Esse equilíbrio é necessário, visto que, a baixa produtividade gerada por uma restrição mais intensa pode afetar consideravelmente a qualidade do serviço médico.

No que se refere ao controle de tentativas de *login*, o sistema deve ser configurável. Esta ação é necessária para permitir que a definição de um número máximo de tentativas consecutivas de autenticação seja realizada e conseqüentemente sendo bloqueado o usuário quando um determinado número de tentativas for atingido.

4.2 Autorização e controle de acesso

No HUSM existe um grande número de funcionários, com diversas funções. Médicos, residentes, “doutorandos” (alunos dos últimos semestres do curso de medicina), enfermeiros, farmacêuticos, etc. Soares (2006) verificou a hierarquia de perfis de acordo com a estrutura organizacional do HUSM (vide tabela 3).

São condições impostas aos perfis para manipulação de prescrições:

- Médicos Assistentes têm acesso irrestrito para ver prescrições, desde que de seus pacientes assistidos;
- Paramédicos só podem ver prescrições de pacientes por eles assistidos, ou sob delegação, desde que os pacientes estejam internados;
- Médicos e Paramédicos podem ver as prescrições de pacientes em atendimento na emergência, desde que o acesso seja durante seu turno de trabalho e através de computadores lotados neste setor;
- Pacientes podem ver exclusivamente as próprias prescrições.

Para funções relacionadas à tecnologia da informação, o manual de certificação exige que o sistema suporte os papéis de gestor de segurança, auditor, administrador do sistema, operador de sistema. Especificamente para a exportação de dados e realização de backup, o sistema de gerenciamento de banco de dados deverá possuir um perfil específico para essa função (operador de backup).

Tabela 3 - Níveis hierárquicos do HUSM. (Soares, 2006)

Usuário	Profissional	Médico	Residente			
			Cirurgião			
			Anestesista			
			Hematologista			
		Paramédico	Enfermeiro	Auxiliar de Enfermagem		
			Psicólogo			
			Fisioterapeuta			
			Biólogo			
			Fonoaudiólogo			
			Dentista			
			Assistente Social			
			Professor de Educação Física			
			Físico			
			Bioquímico			
			Biomédico			
			Farmacêutico	Auxiliar de Farmácia		
			Nutricionista	Auxiliar de Nutrição		
			Auxiliar Técnico			
		Administrador Executivo	Diretor			
			Técnico Administrativo	Auxiliar Administrativo	Escriturário	
					Secretário	
					Auxiliar de Registro de Saúde	Analista de Registro de Saúde
				Técnico em Informações Médico Hospitalares	Analista de Informações Médico Hospitalares	
				Operador de Teleatendimento		
			Administrador de RH	Analista de RH	Auxiliar de RH	
			Administrador Financeiro	Faturista	Analista de Faturamento	
				Técnico Contábil	Analista Contábil	
		Técnico de Informática	Analista de Informática	Analista de Suporte		
				Analista Desenvolvedor		
			Administrador de Banco de Dados			
		Pesquisador	Pesquisador Clínico			
	Paciente					
	Estudante	Graduando				
		Pós-Graduando				

Em sua dissertação, Soares (2006) faz um estudo sobre diferentes modelos de controle de acesso, e propõe um modelo, o *Contextual Information-Based Access Control* (CIBAC). A arquitetura proposta pelo autor é dividida em módulos funcionais (figura 7), separando o mecanismo de controle de acesso dos mecanismos de

atualização, possibilitando uma abordagem genérica do modelo, não o restringindo a apenas uma aplicação.

O Módulo de Controle de Acesso verifica as regras necessárias para o acesso, contidas nas condições de contexto (CC) e confronta os dados com as informações de contexto do sistema (CI), liberando ou não o acesso. Em cada requisição de acesso são necessárias informações relativas às credenciais do usuário, objeto e modo de acesso.

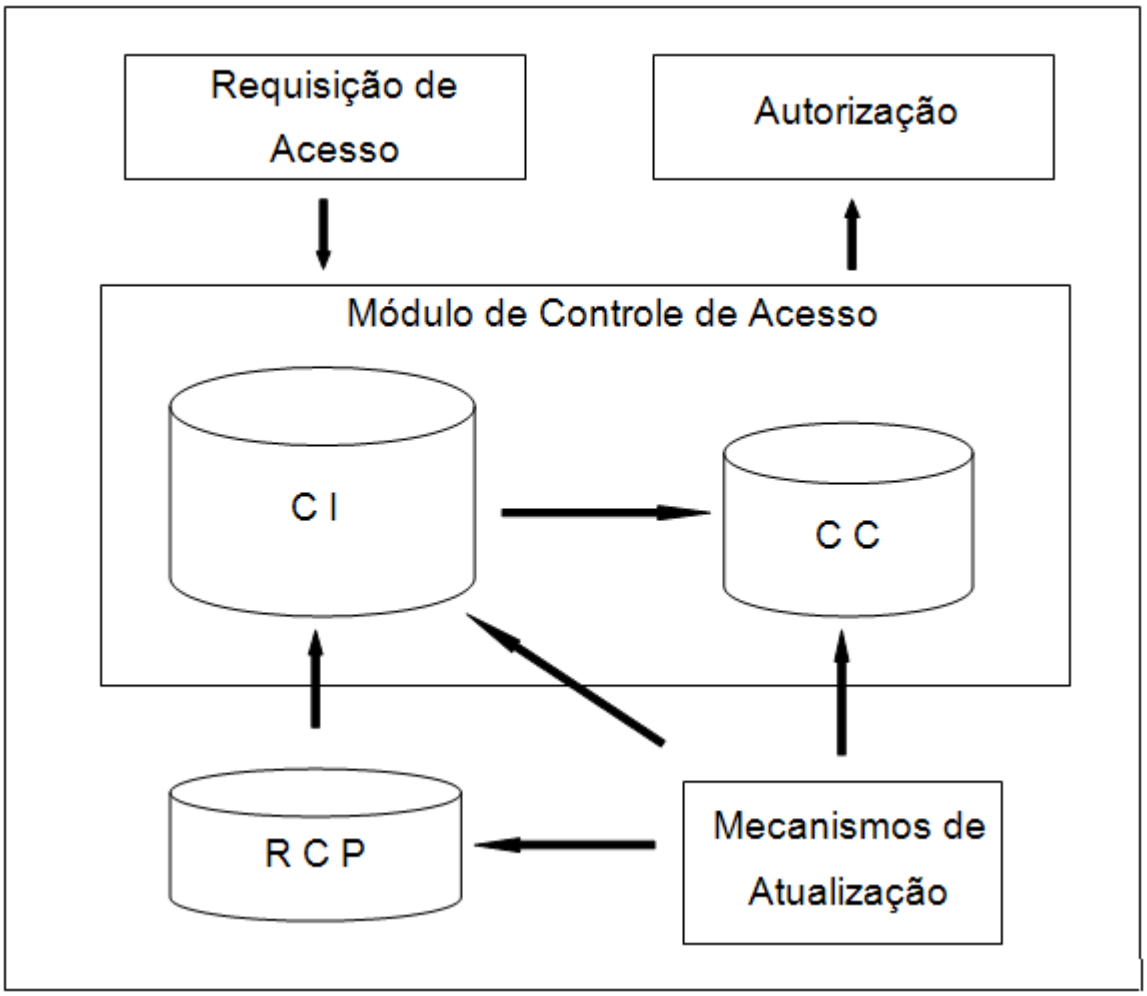

Figura 7 - Arquitetura do CIBAC. (Soares, 2006)

O S-RES não poderá ser acessado de outra maneira a não ser através do controle de acesso, nesse caso através do CIBAC.

4.2.1 Análise Parcial

A autorização e o controle de acesso têm como principal objetivo impedir o acesso a dados por usuários não autorizados. A ação proposta neste trabalho para atender esse controle estabelece o CIBAC (Soares 2006) como solução. O CIBAC provê diferentes formas de acesso a informações em um ambiente hospitalar, propiciando a adequação com a legislação pertinente. A abordagem defendida pelo autor permite a aplicação de políticas e regras de acesso mais específicas, agregando mais funcionalidade aos sistemas de controle de acesso.

A disponibilidade de mecanismos de configuração de controle de acesso, para a implementação da política, é atingida pelo modelo ao possuir o controle de política de acesso armazenado de forma independente.

4.3 Disponibilidade do S-RES

O manual de certificação faz apenas duas exigências nesse quesito. A primeira é que as cópias de segurança dos S-RES contenham, além dos dados, os atributos de segurança. Exige também que em uma restauração, os atributos de segurança, juntamente com os dados, sejam recuperados sem a intervenção adicional de um administrador. Tanto a realização do backup quanto a restauração devem ser operações exclusivas do usuário com perfil operador de backup.

A segunda exigência se refere à verificação de integridade na recuperação dos dados. Quando um backup for realizado, os dados gerados deverão ser conferidos com os originais para garantir a integridade dos mesmos. Na restauração de uma base de dados, o inverso deverá ocorrer. Os dados restaurados do banco deverão ser conferidos com os dados do backup de origem (figura 8).

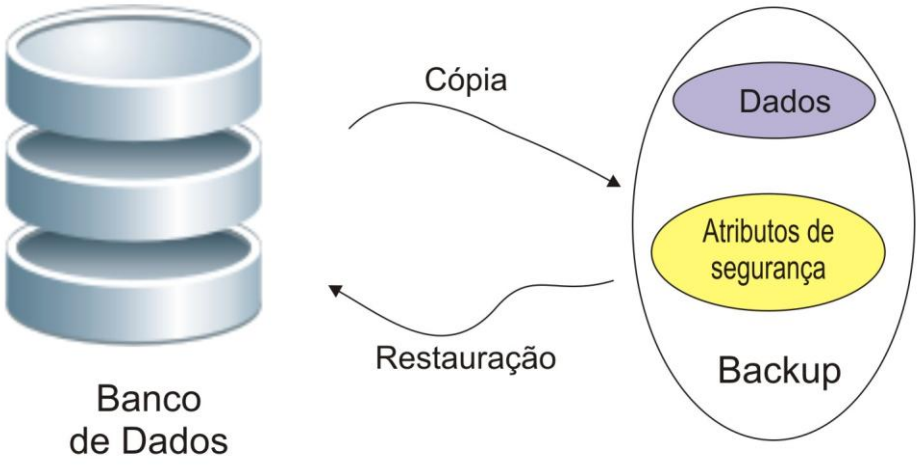

Figura 8 - Realização e restauração de backup

Segundo Narang et al. (2002) todos os bancos de dados comerciais, e a maioria dos gratuitos, possuem ferramentas próprias para a verificação de integridade na realização e restauração de cópias de segurança.

4.3.1 Análise Parcial

Para atender esse requisito o próprio Manual de Segurança para S-RES é superficial. As poucas exigências estabelecidas podem ser cumpridas pelos sistemas gerenciadores de banco de dados, ficando a disponibilidade do sistema presa à intervenção de algum usuário para a realização da restauração do sistema.

A disponibilidade pode ser considerada um dos principais princípios essenciais para a segurança da informação, isto por que se a disponibilidade dos dados não for garantida os outros princípios passam a não existir. Desta maneira o Manual de Segurança para S-RES poderia fazer maiores exigências para os sistemas, garantindo assim níveis mais efetivos para que a disponibilidade seja uma prioridade. Uma simples cópia de segurança mantida em local diferente ao do sistema garante a preservação dos dados em casos extremos como incêndios ou inundações, mas pode ser necessário muito mais.

4.4 Comunicação Remota

Em ambientes conectados, a necessidade de transportar informação de um lugar para outro é comum. Segundo o Manual de Segurança para S-RES, é mandatório que a comunicação entre o cliente e o servidor seja segura, garantindo a integridade e confidencialidade dos dados. A preocupação é como transportar informações de uma maneira segura uma vez que os dados trafegam por zonas que, mesmo sob o controle das empresas, possam ser vítimas de vazamento de informações. Uma solução é a utilização de *Virtual Private Networks (VPN)* (Northcutt et al., 2005).

O conceito básico de *VPN* é garantir a segurança de canais de comunicação com criptografia. Esta pode ser obtida em diferentes camadas da rede: aplicação, transporte, rede e enlace (figura 9).

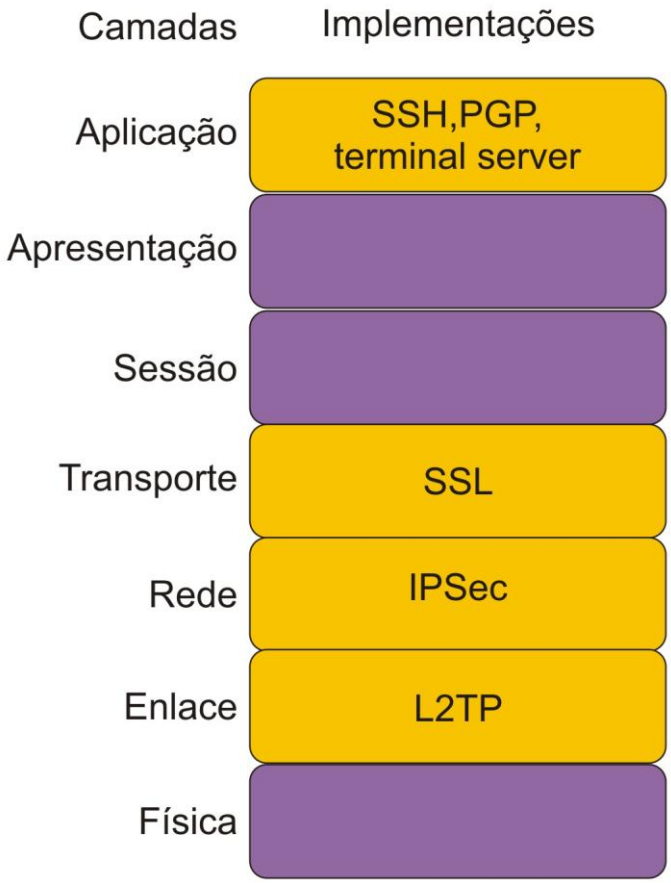

Figura 9 - Implementações de VPN em diferentes camadas de rede

Na camada de aplicação, criptografia pode ser aplicada com programas como o *Pretty Good Privacy* (PGP) ou através de canais como *Secure Shell (SSH)*. Ainda, programas como o *pcAnywhere* e *Terminal Server* podem ser usados com criptografia para proteger comunicações remotas.

Na camada de transporte, protocolos como *Secure Sockets Layer (SSL)* podem ser utilizados para proteger o conteúdo de uma comunicação específica entre duas partes. *SSL* são tipicamente utilizados em navegadores *web* (Canvel et al., 2003).

Na camada de rede, protocolos como IPSec fazem a criptografia não somente dos dados transmitidos mas também das informações TCP/IP (RFC 4301). Embora a informação do endereço IP seja importante para o roteamento dos pacotes, informações de alto nível, como protocolos de transporte e portas associadas podem ser ofuscadas.

Layer 2 Tunneling Protocol (L2TP) é um complemento ao *Point-to-Point Protocol (PPP)*, que permite a criptografia de pacotes enviados via *PPP* na camada de enlace.

O método mais utilizado para a construção de *VPN*s é o *SSL* baseado na *web*. Inúmeras páginas na internet utilizam *SSL* para fornecer conexão segura entre navegadores e servidores. A maioria dos usuários não toma conhecimento da utilização do *SSL* a não ser pelo cadeado que pode ser visto, como na figura 10, em um navegador quando a conexão é utilizada (Canvel et al., 2003). Um tráfego padrão *HTTP* utiliza a porta *TCP* 80, já um *HTTP* criptografado com *SSL* (também conhecido como *HTTPS*) utiliza a porta *TCP* 443.

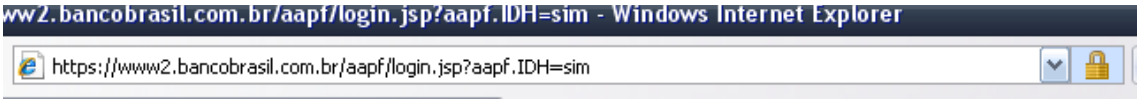

Figura 10 - Utilização de SSL em uma página web

O sistema também deverá prever um cadastramento de máquinas habilitadas para sua utilização. Somente máquinas cadastradas no sistema terão acesso à página de login. Acessos provenientes de outros computadores deverão ser bloqueados, delimitando assim o perímetro de utilização do sistema.

A conexão entre o S-RES e o sistema de banco de dados deverá garantir a autenticação dos dispositivos, bem como a integridade e confidencialidade dos

dados em trânsito. Depois de definir quais endereços IP terão acesso ao sistema de banco de dados, provavelmente apenas um endereço, o IP do servidor rodando a aplicação da prescrição eletrônica, deve-se bloquear o acesso ao banco de dados para todos os outros endereços.

Segundo Natan (2005) bancos de dados nunca devem ficar expostos diretamente a uma rede pública. Para o sistema de prescrição eletrônica do HUSM não há razão para que a base de dados fique exposta dessa forma, pois o servidor *web* será o único a realizar conexões diretamente com o banco de dados. Pode-se proteger o banco de dados de acesso externo utilizando a arquitetura da figura 11.

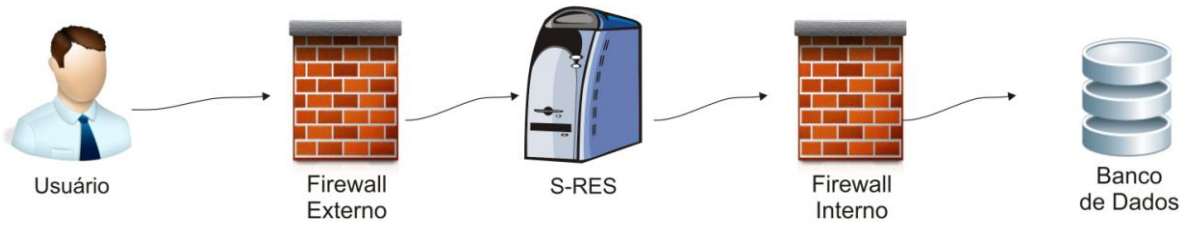

Figura 11 - Banco de dados sem acesso externo

4.4.1 Análise Parcial

A comunicação remota representa uma grande fonte de possíveis intervenções de usuários malfeitores. Uma das soluções que prevê a autenticação do cliente e a integridade dos dados pode ser obtida com a utilização de *SSL*.

Por não existir uma preocupação de configuração em clientes e ser um padrão para aplicações *web*, a utilização de *SSL* na comunicação cliente-servidor é recomendada para o sistema de Prescrição Eletrônica do HUSM.

Outro ponto importante a ser destacado é a correta configuração de *firewalls* para o sistema. Somente IPs cadastrados poderão ter acesso ao S-RES e apenas o servidor de aplicação poderá ter acesso a base de dados. Esta estratégia não só garante que apenas componentes autorizados realizem a comunicação entre si, como também estabelece um controle de segurança importante em se tratando de uma unidade hospitalar de grande porte como o HUSM, onde máquinas e responsáveis pelo serviço podem estar em locais distintos.

4.5 Segurança de dados

4.5.1 Impedimento de exclusão e alteração

Uma exigência nesse item do manual de segurança é que nenhum dado pode ser alterado ou removido do sistema. Ações de correção deverão preservar os dados antigos. Ou seja, em uma tabela de prescrições, caso haja necessidade de alterar alguma informação, a nova informação não poderá sobrescrever a antiga. Para isso, uma nova tupla deverá ser gravada, e a antiga pode ser definida como inválida, invisível ou até mesmo movida para outra tabela, mas mesmo assim mantida no sistema. Desta forma, podem-se comparar as versões e saber que alterações foram feitas em uma futura auditoria.

Essa segurança de dados pode ser controlada pela aplicação ou pelo próprio gerenciador de banco de dados. Quando for controlada pela aplicação, deve-se notar os seguintes: a complexidade do desenvolvimento aumenta, visto que o sistema deverá se preocupar em registrar todas as alterações realizadas, e se algum usuário tiver acesso diretamente ao banco de dados, poderá fazer qualquer alteração nos dados pois não passará por nenhum controle implementado e conseguirá realizar operações no banco sem que elas fiquem registradas.

Já um controle implementado diretamente no gerenciador de banco é utilizado de maneira transparente para o sistema, o banco será o responsável em manter os dados em sua base, sem que o sistema saiba. Caso um usuário tenha acesso diretamente ao banco, novamente passando por cima da aplicação, toda ação executada por ele ficará registrada da mesma forma.

Uma maneira de não permitir que dados sejam excluídos ou alterados na camada do gerenciador do banco de dados é com a utilização de gatilhos (*triggers*). Um gatilho deve ser definido para cada tabela e para cada ação (podendo também ser definido um gatilho para mais de uma ação). Outra configuração necessária é definir se o gatilho será disparado antes, depois ou ao invés da ação solicitada pelo usuário.

Como exemplo, em um caso onde um médico deseja alterar o peso de um paciente. A tabela PACIENTE possui os campos ID, NOME e PESO. Para manter o registro de todas as alterações realizadas nessa tabela, cria-se outra chamada PACIENTE_LOG com as colunas ID, NOME, PESO, DATA_ALTERACAO. Para criar

o gatilho responsável em registrar qualquer alteração na tabela PACIENTE tem-se o código da figura 12.

Assim, toda vez que um comando UPDATE ou DELETE for executado na tabela PACIENTE, o próprio banco de dados, sem que o usuário ou a aplicação saibam ou necessitem se preocupar, irá gerar um registro na tabela PACIENTE_LOG que conterá o dado antigo. Dessa forma, através de comparações entre os dados chega-se às alterações realizadas.

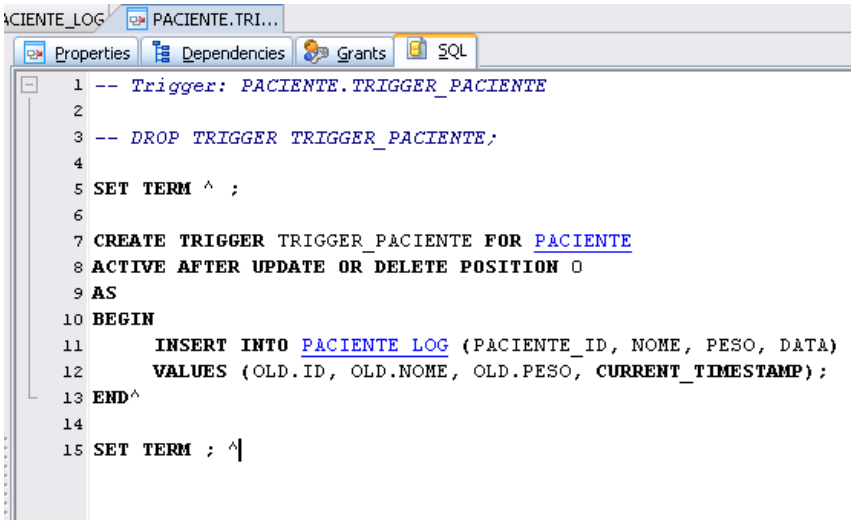

Figura 12 - Criação de gatilho para registrar alterações na tabela Paciente

Algo importante a ser notado nesse ponto é que não há um registro de que usuário realizou essa alteração. Esse registro deverá ser feito em um *log* da aplicação.

Em uma seqüência de execuções como as da tabela 6, novos pacientes são inseridos na tabela PACIENTE (tabela 4). No momento em que alterações nessa tabela acontecem, os dados antigos são copiados para outra tabela, PACIENTE_LOG (tabela 5), e os novos dados sobrescrevem os antigos. Quando uma operação de remoção é executada, os dados são movidos da tabela PACIENTE para a PACIENTE_LOG.

Dadas a seqüência de execuções da tabela 6, as tabelas ficarão da seguinte forma:

Tabela 4 - Tabela PACIENTE após operações realizadas

ID	NOME	PESO
1	Francisco	80
2	Henrique	100
4	Ripoli	60

Tabela 5 - Tabela PACIENTE_LOG após operações realizadas

ID_PACIENTE	NOME	PESO	DATA_ALTERACAO
1	Francisco	50	DATA( )
1	Francisco	65	DATA( )
2	Henrique	120	DATA( )
3	Caio	40	DATA( )

Tabela 6 - Tabela de operações

Insere	paciente 1	nome Francisco	peso 50
Insere	paciente 2	nome Henrique	peso 120
Altera	paciente 1	nome Francisco	peso 65
Insere	paciente 3	nome Caio	peso 40
Altera	paciente 1	nome Francisco	peso 80
Altera	paciente 2	nome Henrique	peso 100
Remove	paciente 3		
Insere	paciente 4	nome Ripoli	peso 60

4.5.2 Dados de identificação do paciente criptografados

Outra exigência do manual de certificação é a criptografia dos dados de identificação do paciente. Caso a base de dados tenha seu acesso violado, através de acesso não autorizado, a criptografia deverá impedir que qualquer histórico médico do paciente seja reconstruído.

A criptografia dos dados guardados em um banco de dados funciona como

uma camada adicional de segurança para dados sigilosos que necessitam de uma proteção maior que outros.

Segundo Natan (2005) existem dois casos onde os benefícios da criptografia no banco de dados são facilmente reconhecidos. O primeiro caso acontece quando um usuário está olhando para dados que ele não deveria estar vendo, apesar de ter acesso legítimo aos dados. Um exemplo é um administrador de banco de dados (DBA).

Um DBA tem o poder de executar qualquer ação em qualquer tabela do banco. Nas definições de controle de acesso, ele tem poder total e poderia, até mesmo, remover trechos de trilhas de auditoria para ocultar alguma ação indevida.

Ainda segundo Natan (2005), o segundo caso onde a criptografia no banco de dados pode ser útil é quando um roubo de disco ou arquivos ocorre. Mesmo possuindo o melhor controle de acesso no banco de dados, um invasor pode copiar arquivos ou até mesmo o disco inteiro. Em ambos os casos, o do DBA e o do invasor, a criptografia atua como uma importante proteção para os dados.

A criptografia pode ser aplicada em três níveis distintos: na camada de aplicação, na camada de sistema de arquivos, e no próprio banco de dados (figura 13). Quando realizada na camada de aplicação, os desenvolvedores utilizam de ferramentas de criptografia para criptografar e descriptografar os dados. Sistemas desenvolvidos em Java podem utilizar da *Java Cryptographic Extensions (JCE)*, uma API que, entre outras funcionalidades, provê algoritmos para criptografar e descriptografar dados.

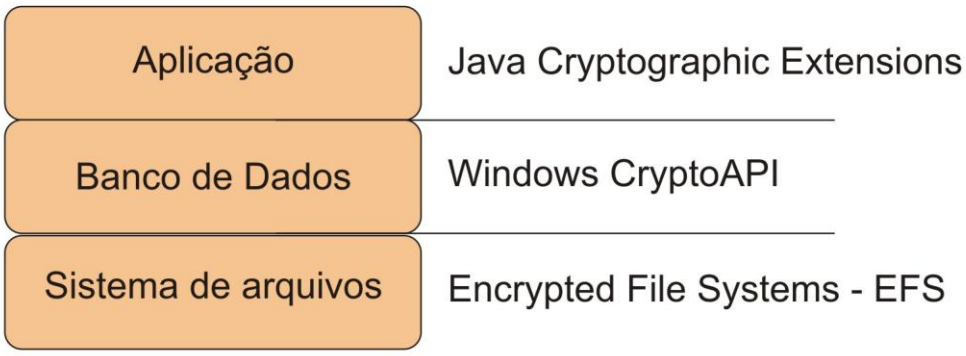

Figura 13 - Criptografia aplicada em diferentes camadas do sistema

Nenhuma configuração no banco de dados é necessária nessa abordagem, sendo transparente para o gerenciador do banco. A única preocupação que se deve ter é com o tamanho das colunas no banco, visto que o dado criptografado precisa de uma coluna de tamanho maior do que um dado limpo.

Entretanto essa abordagem possui algumas desvantagens que faz com que poucos sistemas a adotem (Mattsson, 2005). Como a criptografia acontece na camada de aplicação, o código para criptografar e descriptografar poderá ter que ser escrito em diversos locais, usando diferentes bibliotecas, tornando a solução difícil de implementar e manter. A utilização dos dados criptografados fica restrita à aplicação, por exemplo, uma ferramenta de gerenciamento de banco de dados não poderá ser usada.

A realização de criptografia na camada de sistema de arquivos normalmente acontece quando existem recursos do sistema operacional para o armazenamento no disco de modo criptografado. Um exemplo é o sistema de arquivos *Encrypted File Systems (EFS)*, que pode ser implementado no Windows para criptografar arquivos de dados em um disco usado pelo *SQL Server*.

Problemas com essa abordagem incluem uma diminuição na performance do sistema, pois tudo precisa ser descriptografado antes de ser utilizado. Outra questão é que a criptografia no sistema de arquivos só resolve o caso de roubo de discos do banco porque todo o acesso é feito pelo processo do servidor SQL e, apesar de os dados estarem criptografados pelo sistema operacional, no banco de dados eles não estão.

A terceira opção de criptografia é a implementada diretamente pelo banco de dados. Esse método inclui a utilização de rotinas já pertencentes ao banco e extensões que podem ser adicionadas (Natan, 2005). Essa abordagem restringe a quantidade de sistemas de bancos de dados possíveis de ser utilizados, principalmente quando a solução pretende utilizar um banco *open-source*.

Sesay et al. (2005) propõe um modelo de três camadas para o suporte de criptografia no banco de dados (figura 14). A primeira camada é a interface com o usuário que contém dois blocos: um para usuários de nível baixo (L1) e outro para usuários de nível alto (L2). Os objetos no banco de dados são classificados em públicos (classificados e não classificados) e privados. Todos os usuários têm acesso aos seus dados privados e aos dados públicos não classificados, enquanto que aqueles no nível L2 possuem acesso a dados classificados e não classificados.

Todos os usuários possuem uma chave única, Kp, que é utilizada quando se acessa seus próprios dados privados.

A segunda camada é a de gerência de banco de dados, composta por um bloco de sistema, o *mandatory access control (MAC)*, e outro bloco que contém um controlador (KC) e um *trusted subject (TS)*. O KC é responsável por gerar e manter dois conjuntos de chaves para criptografia, uma Kp para os dados pessoais de cada usuário e Kj para dados públicos classificados. Ele também criptografa dados sigilosos antes de serem armazenados no banco, e descriptografa dados antes de responder consultas dos usuários. O TS é responsável por gerenciar usuários, objetos e seus privilégios.

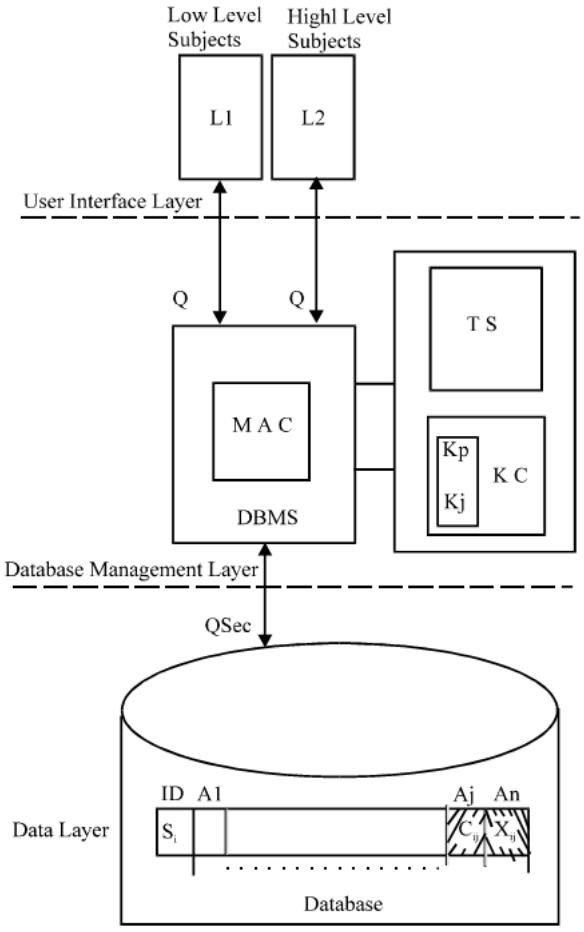

Figura 14 - Modelo para criptografia de dados proposto por Sesay et al. (2005)

Por último, tem-se a camada do banco de dados. Este mantém dados públicos não classificados em texto claro (não criptografado), e dados classificados e privados são armazenados com criptografia. Este modelo de criptografia na base de

dados se mostrou ser eficiente por prover um alto nível de segurança e ao mesmo tempo minimizando o tempo gasto na (des)criptografia (Sesay et al., 2005).

Demonstrado no item 4.2, o CIBAC (Soares, 2006) é a arquitetura de controle de acesso recomendada por este trabalho. Desenvolvida com o foco em sistemas de saúde, o CIBAC pode receber novas funcionalidades, substituir o MAC na arquitetura de Sesay et al. (2005) e possibilitar uma melhor adequação à realidade do HUSM.

4.5.3 Outros requisitos de segurança de dados

O sistema de banco de dados deverá possuir controles para verificação de integridade dos dados RES de forma a prevenir que qualquer ação do usuário ou falha do sistema possa originar uma inconsistência nos dados.

O sistema de prescrição eletrônica não deve permitir acesso direto ao banco de dados pelos usuários. O acesso de usuários ao sistema deve ser permitido somente por intermédio do CIBAC, e nunca diretamente ao SGBD, exceto nas atividades de backup de dados.

4.5.4 Análise Parcial

A segurança dos dados tem como principal preocupação garantir a integridade e a confidencialidade de qualquer informação do paciente. O impedimento de alteração ou exclusão dos dados permite o controle sobre todos os dados que existem ou existiram no banco de dados. Esta restrição é garantida pela utilização de gatilhos ao qual é transparente ao sistema, tanto para os programadores da aplicação, quanto para possíveis usuários que tenham acesso diretamente ao banco de dados.

A criptografia dos dados de identificação do paciente é outro requisito chave do Manual de Segurança para S-RES. Funcionando como mais uma camada de segurança sobre os dados, a criptografia objetiva impede a reconstrução de histórico médico do paciente. Utilizando uma abordagem semelhante a de Sesay et al. (2005), pode-se empregar a camada de aplicação como responsável pela criptografia de

dados de identificação e pelo gerenciamento de chaves para as transformações dos dados.

4.6 Auditoria

Como citado na seção 4.2, o sistema deverá conter um usuário auditor. Ele deverá ser o único com acesso às trilhas de auditoria. Estas trilhas não podem ser modificadas por nenhum usuário e o sistema deverá registrar acesso e modificação de dados.

A modificação de qualquer dado já é registrada com a utilização de gatilhos, mas, com o registro no nível do banco de dados onde toda conexão da aplicação com o banco é realizada da mesma forma, não existe uma distinção de que usuário está realizando a operação. Desta forma, o sistema necessita registrar as ações de usuários na camada de aplicação, ou seja, um registro pelo próprio sistema de prescrição eletrônica sobre toda ação do usuário. Tentativas de autenticação, atividades de gerenciamento do sistema, atividades de operação pelos usuários, enfim, tudo o que puder ser registrado, deverá ser.

O registro deverá conter o nome do usuário que realizou a operação, bem como o endereço IP de acesso, e a data e hora. Esse registro é normalmente mantido em arquivos de *log* do próprio servidor *web* (figura 15), mas também pode ser armazenado em uma tabela específica do banco de dados. Para garantir que a tabela não sofrerá alterações, pode-se utilizar gatilhos, da mesma forma utilizada para garantir a segurança dos dados, e, como na figura 16, criptografia (Waters *et. al*, 2004). Desta forma, somente o usuário auditor terá acesso aos *logs* do sistema.

```
2008-06-16 16:37:05,828 DEBUG [br.gmicro.web.UsuarioLoginController] - user: xico - Entrando no metodo 'formBackingObject'...
2008-06-16 16:37:05,921 DEBUG [br.gmicro.web.UsuarioLoginController] - user: xico - No errors -> processing submit
2008-06-16 16:37:05,921 DEBUG [br.gmicro.web.UsuarioLoginController] - user: xico - Entrando no metodo 'onSubmit'...
```

Figura 15 - Registro de log em arquivo pelo servidor *web*

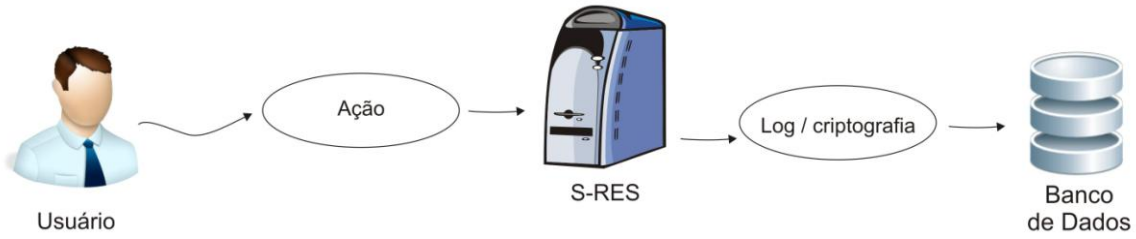

Figura 16 - Registro de ações do usuário gravados, com criptografia, no banco de dados

4.6.1 Análise Parcial

A auditoria é uma dos controles fundamentais para garantir a veracidade das ações realizadas num sistema de prescrição eletrônica. As soluções propostas prevêem a realização da auditoria sempre em dois níveis, na aplicação e diretamente no banco de dados. Os arquivos de *log* do servidor de aplicação deverão registrar com detalhes todas as ações do usuário, indicando data, hora, e local de acesso. Para garantir a confidencialidade, a proteção desse arquivo pode ser feita com a criptografia de cada ação, ou com a utilização de uma base de dados combinada com gatilhos para impedir a alteração de *logs* do sistema.

CONCLUSÃO

Este trabalho apresentou uma proposta de modelo de segurança para prescrição eletrônica do HUSM alinhada com as recomendações contidas no manual de Certificação para Sistemas de Registro Eletrônico em Saúde, avalizada pelo CFM.

O modelo além de contemplar os principais controles determinados no manual, também indica soluções para cada requisito, fundamentados em pesquisas da área, agregando ao manual “o como fazer”, uma vez que o documento não oferece orientação nesse sentido. Esse trabalho não só contribui para uma correta utilização das tecnologias apresentadas, como também a auxiliar na meta requerida para o NGS1, nível foco deste trabalho.

A maior preocupação de um sistema eletrônico de saúde deve ser com a integridade, disponibilidade e confidencialidade dos dados dos pacientes, pois sem esses três pilares de segurança é impossível garantir que o atendimento aconteça conforme a legislação vigente.

Diferentes tipos de autenticação (métodos usuais como usuário e senha, combinado com biometria) garantem que apenas usuários autênticos terão acesso ao sistema. Um controle de acesso baseado em contexto previne, entre outras coisas, que um usuário tenha acesso a dados que não são estritamente necessários.

A transferência de dados de maneira criptografada, com a utilização de *SSL*, entre cliente e servidor, atinge o objetivo de transferir dados de maneira segura, garantindo, principalmente, sua integridade.

A utilização de criptografia no banco de dados garante a confidencialidade dos pacientes e não permite que, mesmo que os discos do banco de dados sejam roubados, um invasor possa reconstruir um histórico médico.

A implantação, o teste e a validação desse modelo são trabalhos futuros que acontecerão à medida que o sistema de prescrição eletrônica ganhar força. Mais adiante, uma extensão deste trabalho para que o sistema se encaixe no NGS2 deve ser outro trabalho possível.

Outro ponto que pode ser ampliado é a questão de disponibilidade. O manual de certificação faz apenas pequenas exigências nesse quesito e com todas as possibilidades tecnológicas existentes um nível mais adequado pode ser atingido.

REFERÊNCIAS

AL-SALQAN, Y. Y. **Security and Confidentiality in Healthcare Informatics**, 7th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Proceedings, p. 371-375, 1998.

BATES, D. W. **Improving medication safety across institutions**. Journal on Quality Improvement 2000; 26(6):319-20, 2000.

BERGER, R. G.; KICHAK, J.; PCHAK, B.A. **Computerized physician order entry: helpful or harmful?** Journal Am Med Inform Assoc, 11:100–3, 2004.

BEZNOSOV, K. **Engineering access control for distributed enterprise applications**. Florida International University, Miami, Florida, EUA, 2000.

BLOBEL, B; ROGER-FRANCE, F. **A systematic approach for analysis and design of secure health information systems.** International Journal of Medical Informatics 62, 51-78, 2001

BRASIL, Ministérios da Educação e da Saúde. **Portaria Interministerial nº. 1000, de 15/04/2004**. Publicada no Diário Oficial da União em 16/04/2004.

CANVEL, B.; HILTGEN, A. P; VAUDENAY, S; VUAGNOUX, M. **Password Interception in a SSL/TLS Channel, Advances in Cryptology** – CRYPTO 2003, 2003.

CFM – Conselho Federal de Medicina; SBIS – Sociedade Brasileira de Informática em Saúde. **Manual de Certificação para Sistemas de Registro Eletrônico em Saúde**, Versão 3, 2007.

CFM - Conselho Federal de Medicina. **Resolução 1.638 e 1.639**. Disponível em: http://www.arnaut.eti.br/ResoCFM.htm, acesso em Ago/2008, 2002.

CFM - Conselho Federal de Medicina. **Resolução 1.821**. Disponível em: http://www.sbis.org.br/, acesso em Ago/2008, 2007.

CFM - Conselho Federal de Medicina. **Resolução 1.246/88**. Código de Ética Médica. 3° ed. Brasília, DF, 1996.

COULOURIS, G.; DOLLIMORE, J; KINDBERG, T. **Distributed Systems: Concepts and Design**, Addison Wesley, Fourth Edition, 2005.

FRANÇA, G. V. **Fundamentos legais e filosóficos do segredo médico**. Revista Electrónica de Derecho y Bioética, 2002.

FRANCISCONI, C. F.; GOLDIM, J. R. **Aspectos bioéticos da confidencialidade e privacidade**. Iniciação à Bioética. Brasília: Conselho Federal de Medicina, 1998.

GIMENES, F. R. E.; MIASSO, A. I.; LYRA JUNIOR, D. P.; GROU, C. R. **Prescrição Eletrônica como fator contribuinte para segurança de pacientes hospitalizados**. Pharmacy Practice, 2006.

JAIN, A. K.; PANKANTI, S; PRABHAKAR, S; HONG, L; ROSS, A; WAYMAN, J. L. **Biometrics: A Grand Challenge**. Proceedings of International Conference on Pattern Recognition, Cambridge, UK, 2004.

Juramento de Hipócrates, http://www.gineco.com.br/jura.htm, acessado em 15 de agosto de 2008, 2004.

KENT, S; SEO, K. **Security Architecture for the Internet Protocol**, RFC 4301, 2005.

KFOURI NETO, M. **Responsabilidade Civil do Médico.** 5ª. Ed. Revista dos Tribunais. São Paulo, 2003.

KOBAYASHI, L. O. M. **Segurança em informações médicas: visão introdutória e panorama atual**, Revista Brasileira de Engenharia Biomédica, v. 23, n. 1, p 53-77, 2007.

MATTSSON, U. **Database Encryption - How to Balance Security with Performance**, ITtoolbox Database: http://hosteddocs.ittoolbox.com/UM070805.pdf. Acesso em Novembro de 2008, 2005

MOTTA, G. H. M. B.; FURUIE, S. S. **Um modelo de autorização contextual para o controle de acesso baseado em papéis.** II Workshop em Segurança de Sistemas Computacionais, Porto Alegre-RS, Brasil. SBC, 2002.

NAKAMURA, E. T; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos.** Editora Berkeley, São Paulo, Brasil, 2007

NARANG, I; MOHAN, C; BRANNON, K; SUBRAMANIAN, M. **Coordinated Backup and Recovery between Database Management Systems and File Systems** - IBM Research Report, RJ10231, 2002

NATAN, R. B. **Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server, DB2 UDB, Sybase**, Digital Press, Newton, MA, 2005

NATIONAL ACADEMY OF SCIENCES. **For the record: protecting electronic health information**. Washington, DC: National Academy Press, 1997.

NBR ISO/IEC 17799:2005 – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2005.

NBR ISO/IEC 27001:2006 – Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2006.

NEUMANN, P. G., **Risks to the Public**, ACM SIGSOFT Software Engineering Notes, v. 30, 2005.

NORTHCUTT, S; ZELTSER, L; WINTERS, S; KENT, K; RITCHEY, R. W. **Inside Network Perimeter Security**, 2005

OLIVEIRA, J. A. P. **Sigilo ou segredo médico: a ética e o direito**. Revista Bioética, Brasília, DF, v. 9, n. 2, p. 141-148, 2001.

Organização das Nações Unidas, **Declaração Universal dos Direitos Humanos, 1948**, http://www.unhchr.ch/udhr/lang/por.htm, acessado em 15 de agosto de 2008, 2004.

PFLEEGER, C. P. **Security in computing**, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 1997.

RENAUD, K. **Quantifying the quality of web authentication mechanisms: a usability perspective**. Journal of Web Engineering, 2004.

RIDLEY, A. S.; BOOTH, S. A.; THOMPSON C. M.; **Prescription errors in UK critical care units**. Anaesthesia, 59: 1193-200, 2004.

RINDFLEISCH, T. C. **Privacy, information technology and health care**. Communications of the ACM, v. 40, n. 8, p. 93-100, ago. 1997.

SACARDO, D. P.; FORTES, P. A. C. **Desafios para a preservação da privacidade no contexto da saúde**. Revista Bioética, Brasília, DF, v. 8, n. 2, p. 307-322, 2000.

SESAY, S; YANG, Z; CHEN, J; XU, D; **A Secure Database Encryption Scheme, Second IEEE Consumer Communications and Networking Conference 2005**, 2005.

SMITH, E.; ELOFF, J.H.P. **Security in health-care information systems – current trends**, International Journal of Medical Informatics, 1999.

SOARES, G. A. **Utilização de informações contextuais em um modelo de controle de acesso a informações médicas**. Dissertação, Universidade Federal de Santa Maria, 2006.

VARGA, A. C. **The Main Issues in Bioethics.** Paulist Press, USA. 1980.

WATERS, B. R; BALFANZ, D; DURFEE, G; SMETTERS, D. K. **Building an encrypted and searchable audit log**. Proceedings of 11th Annual Network and Distributed System, 2004.

WILLIAMS, P. A. H. **The role of standards in medical information security: An opportunity for improvement**. The 2006 International Conference on Security & Management. Las Vegas, Nevada, USA, 2006.

WINTERSTEIN, A. G.; THOMAS E; ROSENBERG, E. L.; HATTON, R. C.;

GONZALEZ, R. R.; KANJANARAT, P. **Nature and causes of clinically significant medication errors in a tertiary care hospital**. American Journal of Health-System Pharmacy, 2004.